Homework 1

Mark Schulist

1)

$$a, b, c \in \mathbb{Z} \tag{1}$$

1.a)

$$a, b > 0 \tag{2}$$

Show that if $a|b$ then $a \leq b$

Proof. From the definition of "divides", we know that $b = ak$ for some $k \in \mathbb{Z}$. We know that $a, b > 0$, so $k > 0$ as well. We can see from the definition of "divides" that multiplying a by a non-negative integer will yield a number larger than or equal to a. Therefore $b \geq a$. □

1.b)

$$a|b \quad a|c \tag{3}$$

Show that $a|bx + cy$ for any $x, y \in \mathbb{Z}$.

Proof. WTS: $[bx + cy = ak]$

We again recall the definition of "divides."

$$b = ak \quad c = al \tag{4}$$

We can multiply the equations by a constant.

$$bx = akx \quad cy = aly \tag{5}$$

And add the two equations.

$$\begin{aligned} bx + cy &= akx + aly \\ bx + cy &= a\underbrace{(kx + ly)}_{\text{some integer}} \end{aligned} \tag{6}$$

The RHS is a times some integer, which is what we needed to show. □

1.c)

$n \in \mathbb{Z}$ with $n > 2$. Let $b_1, b_2, ..., b_n \in \mathbb{Z}$. Suppose $a|b_i$ for all $i \leq n$.

Show that for any n integers $x_1, x_2, ..., x_n \in \mathbb{Z}$ we have

$$a \left| \sum_{i=1}^{n} b_i x_i \right. \tag{7}$$

Proof. Using the fact from the previous problem, we can see that this is true. We can do induction on $\mathbb{N}$.

Our base case is that $a \mid b_1 x_1 + b_2 x_2$ (which is true from the previous problem).

Inductive hypothesis: $a \mid b_1 x_1 + ... + b_j x_j$.

$$a \mid b_1x_1 + ... + b_jx_j + b_{j+1}x_{j+1} \tag{8}$$

This is true as a divides all terms up to j by the inductive hypothesis, and a must also divide the final term by the problem statement. If we see the first j terms as a single term that (that a can divide), then we get two terms and the problem reduces to the same problem as part (b).

□

2)

$$(609, 140) \tag{9}$$

$$\begin{aligned} 609 &= 140 \cdot 4 + 49 \\ 140 &= 49 \cdot 2 + 42 \\ 49 &= 42 \cdot 1 + 7 \\ 42 &= 7 \cdot 6 + 0 \end{aligned} \tag{10}$$

So...$\rightsquigarrow (609, 140) = 7$

Solve for $609x + 140y = 7$.

$$\begin{aligned} 7 &= 49 - 42 \\ 7 &= 49 - 140 + 49 \cdot 2 \\ 7 &= -140 + (609 - 140 \cdot 4) \cdot 3 \\ 7 &= -140 + 609 \cdot 3 - 140 \cdot 12 \\ 7 &= 609 \cdot 3 - 140 \cdot 13 \\ \implies x &= 3, y = -13 \end{aligned} \tag{11}$$

3)

$$ax + by = 6 \tag{12}$$

If we let $a = b = 3$, then $3 \cdot 1 + 3 \cdot 1 = 6$. But $(3, 3) = 3$. So this is an example of why (a, b) does not need to be 6.

Similarly, we can show that $a = 4, b = 2$ also works, with $(4, 2) = 2$.

We can also show that $a = 6, b = 1$ works and $(6, 1) = 1$.

And $a = 0, b = 6 = (6, 0) = 6$

This list of GCDs $\{1, 2, 3, 6\}$. As we can see, this list includes all of the divisors of 6.

We can further split this up into *pairs* of divisors of 6, such that the product of each pair equals 6.

For example, $1 \cdot 6 = 6$ and $2 \cdot 3 = 6$.

First we find all of the *factors* of 6, and then we find all of the complements to those factors such that each factor multiplied by the other factor equals 6. Our set of possible GCDs is the set of all factors and their complements.

We can use the next problem to show that our list is complete.

Proof. Let $r = ax + by = 6$. Then we know that we can write $r = (a, b)n$ for some $n \in \mathbb{N}$.

In our example, we have that $6 = (a, b)n$. The possible choices for (a, b) are all of the values that divide 6.

$$(a, b) \in \{x \in \mathbb{N} \mid x|6\} \tag{13}$$

These are also known as the *factors* of 6, which are $\{1, 2, 3, 6\}$, hence showing our list is exhaustive. □

4)

$a, b \in \mathbb{Z}$ not both 0.

$$C(a, b) = \{ax + by \mid x, y \in \mathbb{Z}\} \tag{14}$$

Show $C(a, b) = \{(a, b)n \mid n \in \mathbb{Z}\}$

Proof. To prove that

$$\{ax + by \mid x, y \in \mathbb{Z}\} = \{(a, b)n \mid n \in \mathbb{Z}\} \tag{15}$$

we need to show that each set is contained within the other.

First show that $\{ax + by \mid x, y \in \mathbb{Z}\} \subseteq \{(a, b)n \mid n \in \mathbb{Z}\}$

Suppose $r = (a, b)fx + (a, b)gy \in \{ax + by \mid x, y \in \mathbb{Z}\}$. Then:

$$r = (a, b)\underbrace{(fx + gy)}_{\text{some integer}} \tag{16}$$

Hence, $r \in \{(a, b)n \mid n \in \mathbb{Z}\}$.

Now we can show that $\{(a, b)n \mid n \in \mathbb{Z}\} \subseteq \{ax + by \mid x, y \in \mathbb{Z}\}$.

Suppose $r = (a, b)n$ for some $n \in \mathbb{Z}$.

Then $a = (a, b)x$ and $b = (a, b)y$ for some $x, y \in \mathbb{Z}$.

Add the equations:

$$\begin{aligned} a + b &= (a, b)(x + y) \\ a + b &= (a, b)n \quad \text{let } x + y = n \\ a + b &= r \end{aligned} \tag{17}$$

Hence, $r = a + b$, $r \in \{ax + by \mid x, y \in \mathbb{Z}\}$. □

5)

5.a)

Show $D(a) \cap D(b) = D((a, b))$

Proof. We can show that each set is contained within the other so show they are equal.

WTS: $D(a) \cap D(b) \subseteq D((a, b))$.

For any $x \in D(a) \cap D(b)$, we know that x divides a and b.

We can write $a = xk$ and $b = xl$ because x divides a and b.

$$a = x((k,l)\alpha) \qquad b = ((k,l)\beta) \tag{18}$$

We want to show that $x(k,l) = (a,b)$. AFSOC that $x(k,l) \neq (a,b)$. Then $(\alpha,\beta) > 1$, which constradicts our choice of α and β, which were chosen such that there are coprime.

Hence,

$$(k,l)x = (a,b) \implies x \mid (a,b) \implies x \in D((a,b)) \tag{19}$$

WTS: $D((a,b)) \subseteq D(a) \cap D(b)$

For any $y \in D((a,b))$, we know that y divides (a,b) which must divide a and b by definition (it is the *greatest common divisor*, in other words "divides" is transitive). So $y \in D(a) \cap D(b)$. □

$$a, b, c \in \mathbb{Z} \tag{20}$$

$$(a,b,c) = \max\{D(a) \cap D(b) \cap D(c)\} \tag{21}$$

5.b)

Show that $(a,b,c) = (a,(b,c))$

Proof. We know that intersection is associative.

$$\begin{gathered}(a,(b,c)) = (a,b,c) \\ D(a) \cap (D(b) \cap D(c)) = D(a) \cap D(b) \cap D(c)\end{gathered} \tag{22}$$

Therefore, it does not matter the order in which we apply the GCD "operation," and we can be "lazy" and not write the parentheses. □

5.c)

Proof. Assume there exists $d \in C(a,b,c)$ with $0 < d < (a,b,c)$. $d \in C(a,b,c)$ so there exists $x, y, z \in \mathbb{Z}$ such that $ax + by + cz = d$. We know that $(a,b,c)|a$ and $(a,b,c)|b$ and $(a,b,c)|c$, so by the linear combination proposition, (a,b,c) divides any linear combination of a, b, c. In particular, $(a,b,c)|d$ which implies that $(a,b,c) \leq d$ ↯.

This cannot be true because we assumed that $d > (a,b,c)$, so therefore (a,b,c) must be the smallest positive element in $C(a,b,c)$. □

5.d)

(b) GCD is "associative" (and also commutative) so order of determining divisors does not matter.

(c) $(a_1, a_2, ..., a_n)$ is the smallest element of $C(a_1, a_2, ..., a_n) = \{a_1x_1 + a_2x_2 + ... + a_nx_n \mid x_1, x_2, ..., x_n \in \mathbb{Z}\}$

5.e)

Proof. We can give a counterexample that disproves the statement.

Let $a = 6, b = 10, c = 15$. Then $(a,b,c) = 1$.

But $(a,b) = 2, (a,c) = 3, (b,c) = 5$. □

6)

$N = 8$

1, 2, 1, 4, 1, 2, 1, 8, 1, 2, 1, 4, 1, 2, 1, 8, 1, 2, 1, 4, ...

The period of this sequence is 8 (i.e. there are 8 numbers before it repeats). The period corresponds with my choice of N.

If $N = 7$ (which is prime)

1, 1, 1, 1, 1, 1, 7, 1, 1, 1, 1, 1, 1, 7, 1, 1, 1, 1, 1, 1, ...

The period is 7, which equals N.

If $N = 6$

1, 2, 3, 2, 1, 6, 1, 2, 3, 2, 1, 6, 1, 2, 3, 2, 1, 6, 1, 2, ...

The period is 6.

So it seems like the period is the value of N.

To prove this fact, we would need to use the fact that

$$(a, N) = (N, a - Nk) \tag{23}$$

Everytime we increment k, both sides remain equal but the RHS will "look" different. Incrementing k will make the second argument in the RHS become N larger, which is the period in our sequence.

We also know that the sequence can't repeat in the first N terms, so N is the period and not just an upper bound on the period.

7)

7.a)

Show that $\text{ord}_p(ab) = \text{ord}_p(a) + \text{ord}_p(b)$

Proof. Let $a = p_1^{a_1} p_2^{a_2} p_3^{a_3} ...$ and $b = p_1^{b_1} p_2^{b_2} p_3^{b_3} ....$

Then $ab = p_1^{a_1+b_1} p_2^{a_2+b_2} p_3^{a_3+b_3} ....$

Then $\text{ord}_{p_i}(a) = a_i$ and $\text{ord}_{p_i}(b) = b_i$.

Then $\text{ord}_{p_i}(ab) = a_i + b_i = \text{ord}_{p_i}(a) + \text{ord}_{p_i}(b)$ as the exponents are added when we multiply numbers. □

7.b)

Proof. Let $r_a = \text{ord}_p(a)$ and $r_b = \text{ord}_p(b)$.

WLOG let $r_a \leq r_b$. Then $\min\{r_a, r_b\} = r_a$.

We know from the FTA:

$$a = p^{r_a} l \qquad b = p^{r_b} k \tag{24}$$

Therefore:

$$\begin{aligned} a + b &= p^{r_a} \cdot l + p^{r_b} + k \\ &= p^{r_a}(l + p^{r_b - r_a} k) \quad \text{using } r_a \leq r_b \end{aligned} \tag{25}$$

Therefore the exponent of p must be at least r_a. It could be larger if $p|(l + p^{r_b - r_a} k)$, but it does not necessarily need to be.

Hence, $\text{ord}_p(a + b) \geq r_a$ where $r_a = \min\{\text{ord}_p(a), \text{ord}_p(b)\}$. □

Example 1

$\text{ord}_p(a + b) = \min\{\text{ord}_p(a), \text{ord}_p(b)\}$ in the following example.

Let $a = 8, b = 16$. Then

$$\text{ord}_2(8 + 16) = \text{ord}_2(24) = 3 \tag{26}$$

And $\text{ord}_2(8) = 3$, $\text{ord}_2(16) = 4$. So $\min\{3, 7\} = 3$

Example 2

$\text{ord}_p(a + b) = \min\{\text{ord}_p(a), \text{ord}_p(b)\}$ in the following example.

Let $a = 9, b = 18$. Then

$$\text{ord}_3(9) = 2 \qquad \text{ord}_3(18) = 2 \tag{27}$$

$$\text{ord}_3(9 + 18) = \text{ord}_3(27) = 3 \tag{28}$$

As we can see, $\min\{\text{ord}_3(9), \text{ord}_3(18)\} = 2$ (they are the same). But this value is less than $\text{ord}_3(27) = 3$. So this is an example of when the LHS is strictly greater than the RHS.

We can also see that in this second example, the ord of a and b were the same, which led to the prime of interest having an additional term in the factorization of their sum.

7.c)

Show that $b \mid a \iff \text{ord}_p(a) \leq \text{ord}_p(b) \forall p \in \{\text{primes}\}$

Proof.

$(\implies)$

We are given that $b \mid a \implies a = bx$ for some $x \in \mathbb{Z}$. Therefore:

$$\begin{aligned} &\text{ord}_p(a) = \text{ord}_p(bx) \\ &\text{ord}_p(a) = \underbrace{\text{ord}_p(b)}_{\geq 0} + \underbrace{\text{ord}_p(x)}_{\geq 0} \\ &\text{ord}_p(a) \leq \text{ord}_p(b) \end{aligned} \tag{29}$$

If we add a non-negative value to the RHS, we cannot get a smaller value than $\text{ord}_p(b)$. We did not assume that p takes on a particular value, so therefore this applied to all prime numbers p.

$(\impliedby)$

Given $\text{ord}_p(b) \leq \text{ord}_p(a)$, show that $b \mid a$.

$$\begin{aligned} a &= p_1^{a_1} p_2^{a_2} \dots \\ b &= p_1^{b_1} p_2^{b_2} \dots \end{aligned} \tag{30}$$

If we "divide" a by b, then we get the following:

$$\frac{a}{b} = p_1^{a_1 - b_1} p_2^{a_2 - b_2} \tag{31}$$

But we know that $\text{ord}_p(b) \leq \text{ord}_p(a)$ for all primes, so the exponents on the RHS must all be positive, which means that the RHS is still an integer. Hence, $b \mid a$. □

7.d)

Proof. Given that $(a,b)|a$ and $(a,b)|b$, by part (c) we know the following 2 statements are true:

$$\text{ord}_p((a,b)) \leq \text{ord}_p(a) \qquad \text{ord}_p((a,b)) \leq \text{ord}_p(b) \tag{32}$$

We want to show that $[\text{ord}_p((a,b)) = \text{ord}_p(a)$ or $\text{ord}_p((a,b)) = \text{ord}_p(b)]$ to prove that the min of them is equal to $\text{ord}_p((a,b))$.

AFSOC that neither of the above are true.

Let $\min\{\text{ord}_p(a), \text{ord}_p(b)\} - \text{ord}_p((a,b)) = k$.

Then we know that $(a,b)k \mid a$ and $(a,b)k \mid b$. But that implies that (a,b) is not the GCD because it is too small (not the smallest divisor of a and b) ↯.

So $\text{ord}_p((a,b)) = \text{ord}_p(a)$ or $\text{ord}_p((a,b)) = \text{ord}_p(b)$. Because $\text{ord}_p((a,b))$ is equal to the lower bounds established in Equation 32, we know that $\text{ord}_p((a,b))$ exactly equals the minimum of $\text{ord}_p(a)$ and $\text{ord}_p(b)$. □

8)

Given $m \mid ab$ and $(a,m) = 1$, show that $m \mid b$.

Proof. We want to show that $m \mid b$ which means that $\text{ord}_p(m) \leq \text{ord}_p(b)$.

First given:

$$m \mid ab \implies \text{ord}_p(m) \leq \text{ord}_p(ab) \tag{33}$$

From Equation 33, we can see the following:

$$\text{ord}_p(m) \leq \text{ord}_p(ab) = \text{ord}_p(a) + \text{ord}_p(b) \tag{34}$$

Second given:

$$(a,m) = 1 \implies \prod p^{\min\{\text{ord}_p(a), \text{ord}_p(m)\}} = 1 \implies \min\{\text{ord}_p(a), \text{ord}_p(m)\} = 0 \tag{35}$$

We have two cases with the minimum in Equation 35.

If $\text{ord}_p(m) = 0$ then $\text{ord}_p(m) \leq \text{ord}_p(b)$ because all terms on the RHS of Equation 34 are non-negative.

If $\text{ord}_p(m) \neq 0$, then $\text{ord}_p(a) = 0$, which means that $\text{ord}_p(b) \geq \text{ord}_p(m)$.

□

I prefer this version of the proof because I have more experience thinking about "factors" of numbers (factoring them) compared to thinking about whether a number divides another number. Just the "dividing" symbol makes it seem somewhat scary in the other version of the proof, but in this version we do not have to deal with such notation. I would give this proof, but first start out with a more intuitive approach to ensure that my students understood what it means to factor a number.